2018-05-24

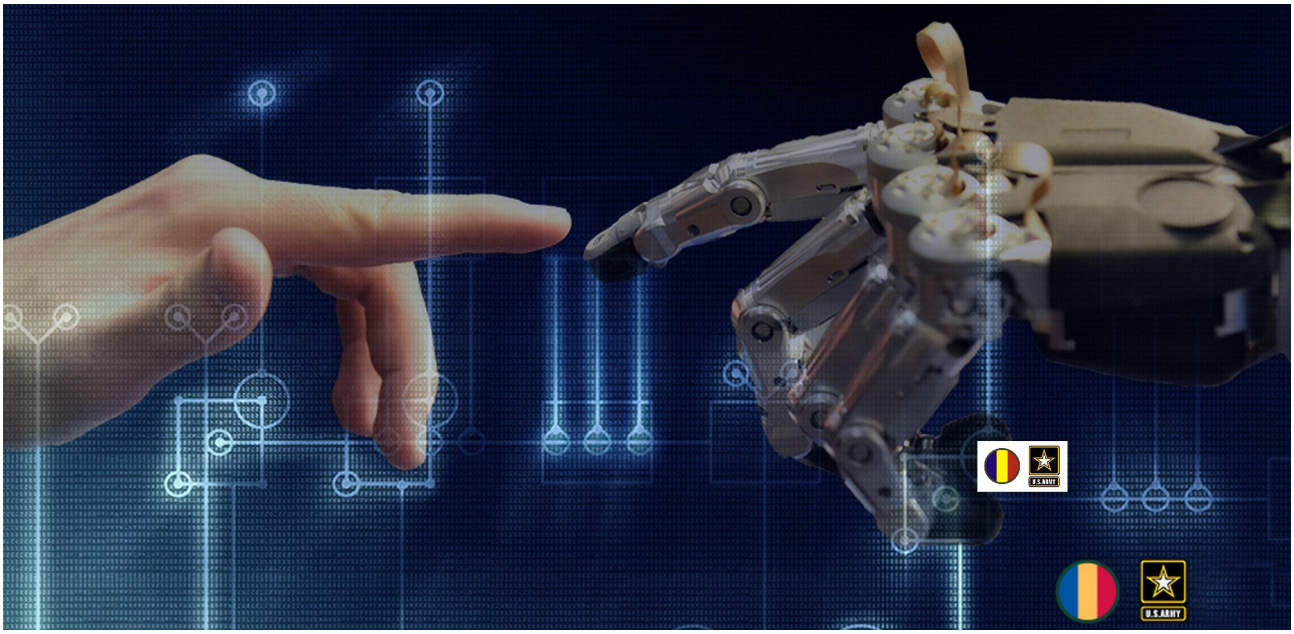
Influence at Machine Speed: The Coming of AI-Powered Propaganda

Telley, Chris

55. Influence at Machine Speed: The Coming of AI-Powered Propaganda

madsciblog.tradoc.army.mil/55-influence-at-machine-speed-the-coming-of-ai-powered-propoganda/

user May 24, 2018



[**Editor's Note:** Mad Scientist Laboratory is pleased to present the following guest blog post by **MAJ Chris Telley**, U.S. Army, assigned to the Naval Postgraduate School, addressing how **Artificial Intelligence (AI)** must be understood as an **Information Operations (IO)** tool if U.S. defense professionals are to develop **effective countermeasures** and **ensure our resilience** to its employment by potential adversaries.]

AI-enabled IO present a more pressing **strategic threat** than the **physical hazards** of **slaughter-bots** or even **algorithmically-escalated nuclear war**. IO are **efforts** to "**influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries**;" here, we're talking about using AI to do so. **AI-guided IO tools** can empathize with an audience to say anything, in any way needed, to **change** the **perceptions** that drive those physical weapons. **Future IO systems** will be able to individually **monitor** and **affect tens of thousands** of people at once. Defense professionals must understand the **fundamental influence potential** of these technologies if they are to drive security institutions to **counter malign AI use** in the information environment.

Programmatic marketing, using consumer's data habits to drive real time automated bidding on **personalized advertising**, has been used for a few years now. **Cambridge Analytica**'s **Facebook** targeting made international headlines using similar techniques, but digital electioneering is just the tip of the iceberg. An AI trained with data from users' social media accounts, **economic media** interactions (Uber, Applepay, etc.), and their devices' **positional data** can **infer predictive knowledge** of its targets. With that knowledge, emerging tools — like **Replika** — can truly befriend a person, allowing it to **train** that individual, for good or ill.

Source: Peter Adamis / Abalinx.com

Substantive feedback is required to **train** an **individual's response**; humans tend to **respond best** to **content** and **feedback** with which they **agree**. That content can be **algorithmically mass produced**. For years, **Narrative Science** tools have helped writers create sports stories and stock summaries, but it's just as easy to use them to **create disinformation**. That's just text, though; today, the **AI** can create **fake video**. A recent warning, ostensibly from former **President Obama**, provides an entertaining yet frightening demonstration of how **Deepfakes** will challenge our **presumptions about truth** in the coming years. The **Defense Advanced Research Projects Agency (DARPA)** is funding a **project** this summer to determine whether **AI-generated Deepfakes** will become impossible to distinguish from the real thing, even using other AI systems.


Source: Getty Creative

Given that **malign actors** can now employ **AI** to **lie** "**at machine speed**," they still have to get the story to an audience. **Russian bot armies** continue to make headlines doing this very thing. The **New York Times** maintains about a dozen Twitter feeds and produces **around 300 tweets a day**, but **Russia's Internet Research Agency (IRA)** regularly puts out **25,000 tweets** in the **same twenty-four hours**. The **IRA's bots** are really just **low-tech curators**; they **collect, interpret,** and **display** desired information to **promote** the **Kremlin's narratives**.

Next-generation bot armies will employ far faster computing techniques and profit from an order of magnitude **greater network speed** when 5G services are fielded. If "**Repetition is a key tenet of IO execution**," then this **machine gun-like ability to fire information** at an audience will, with **empathetic precision** and **custom content**, provide the means to change a decisive audience's **very reality**. No breakthrough science is needed, no bureaucratic project office required. These pieces are **already there**, waiting for an **adversary** to put them together.

Source: Josep Lago/AFP/Getty Images

The DoD is looking at AI but remains focused on **image classification** and **swarming quadcopters** while **ignoring** the **convergent possibilities** of **predictive audience understanding, tailored content production,** and **massive scale dissemination.** What little digital IO we've done, sometimes called social media "**WebOps**," has been **contractor heavy** and **prone** to **naïve missteps**. However, groups like USSOCOM's **SOFWERX** and the students at the **Naval Postgraduate School** are advancing the state of our art. At **NPS**, future senior leaders are working on AI, now. A half-dozen of the school's departments have stood up **classes** and **events** specifically aimed at **operationalizing advanced computing**. The young defense professionals currently working on AI should grapple with **emerging influence tools** and form the **foundation** of the DoD's **future institutional capabilities**.

MAJ Chris Telley *is an Army information operations officer assigned to the Naval Postgraduate School. His assignments have included theater engagement at U.S. Army Japan and advanced technology integration with the U.S. Air Force. Chris commanded in Afghanistan and served in Iraq as a United States Marine. He tweets at @chris_telley.*

This blog post represents the opinions of the author and do not reflect the position of the Army or the United States Government.